HOMELAND SECURITY
COMMITTEE

Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
House Homeland Security Committee

The Role of Cyber Insurance in Risk Management
March 22, 2016

Remarks as Prepared

The House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies meets today to hear from key stakeholders about the role of cyber insurance in managing risk. Just yesterday the Bipartisan Policy Center came out with a publication on the room for growth in this market and the barriers that it faces. Specifically, we hope to hear about the potential for cyber insurance to be used to drive companies of all sizes to improve their resiliency against cyber attacks and develop a more effective risk management strategy, leading to a safer Internet for all Americans.

The cyber insurance market is in its infancy. But it's easy to envision its vast potential. Just as the process of obtaining home insurance can incentivize homeowners to invest in strong locks, smoke detectors, and security alarms, the same could be true for companies seeking to obtain cyber insurance. It is for that reason that I look forward to hearing from the witnesses today on the current state of the cyber insurance market, and what can be done to develop, improve, and expand the availability of cyber insurance in the future.

As news of the recent hacks, breaches, and data exfiltrations demonstrates, cyber vulnerabilities impact every American and cause significant concern. The interconnectedness of society exposes everyone to these risks. The breaches at Home Depot, Target, and JPMorgan Chase are just a few examples of cyber incidents that significantly impacted everyday Americans. Further, according to the World Economic Forum's 2015 Global Risk Report, technological risks in the form of data fraud, cyber attacks, or infrastructure breakdown rank in the top 10 of all risks facing the global economy.

In light of these risks and their enormous significance to individuals, families, and companies, we must explore market-driven methods for improving the security of the companies that store our personal information.

I believe cyber insurance may be one such solution. The very process of considering, applying for, and maintaining cyber insurance requires entities to assess the security of their systems and examine their own weaknesses and vulnerabilities. This process is constructive, not only for obtaining a fairly priced policy, but also as a means of improving the company's security in the process. Obtaining and maintaining cyber insurance may be a market-driven means of enabling "all boats to rise," thereby advancing the security of the nation.

Today, those acquiring cyber insurance largely consist of leading companies that have the most to lose. These market leaders have looked down the road and recognized the best way to mitigate their own vulnerabilities is to insure against as many cyber risks as possible. However, we need to explore ways for this marketplace to expand to create a wide array of diverse, affordable products that will also benefit small and medium-sized entities.

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group has facilitated discussions with relevant stakeholders, including many of the witnesses today, to find ways to further expand the cyber insurance market's ability to address emerging risk areas. The DHS working group has examined the potential value of creating a cyber incident data repository to foster the voluntary sharing of data about breaches, business interruption events, and industrial control system attacks to aid risk mitigation and risk transfer approaches. Additionally, they are looking to develop new cyber risk scenarios, models, and simulations to promote the understanding about how a cyber attack might cascade across infrastructure sections. Lastly, they are examining ways to assist organizations of all sizes in better prioritizing and managing their top cyber risks.

Over the next several decades, I hope to see a matured cyber insurance ecosystem that incentivizes companies of all sizes to adopt stronger cybersecurity best practices and more effective management of cyber risks against bad actors in cyberspace.

We look forward to hearing your perspectives on these efforts and what the private sector is doing to make it easier for Americans to more effectively manage cyber risks. As chairman of this subcommittee, I'm committed to ensuring that legislators help facilitate – but not mandate – solutions to better protect our private sector networks against cyber adversaries. As I see it, the private sector has always led the way with respect to innovation and investment in this space, and we have an obligation to continue leaning heavily on this wealth of front-line expertise.

I have no doubt that this is only the beginning of the conversation on cyber insurance. This market is growing and it is new. I am hopeful that we will continue to find ways to facilitate the healthy, market-driven maturation of the cyber insurance market as an effective means of improving our Nation's cybersecurity posture.

###